TECHNOLOGY TRANSFORMATION SERVICES

SaaS Authorization

July 24th, 2020

Agenda

TECHNOLOGY TRANSFORMATION SERVICES

GSA

1. Objective
2. What we did
3. Findings
4. Next steps
5. Discussion

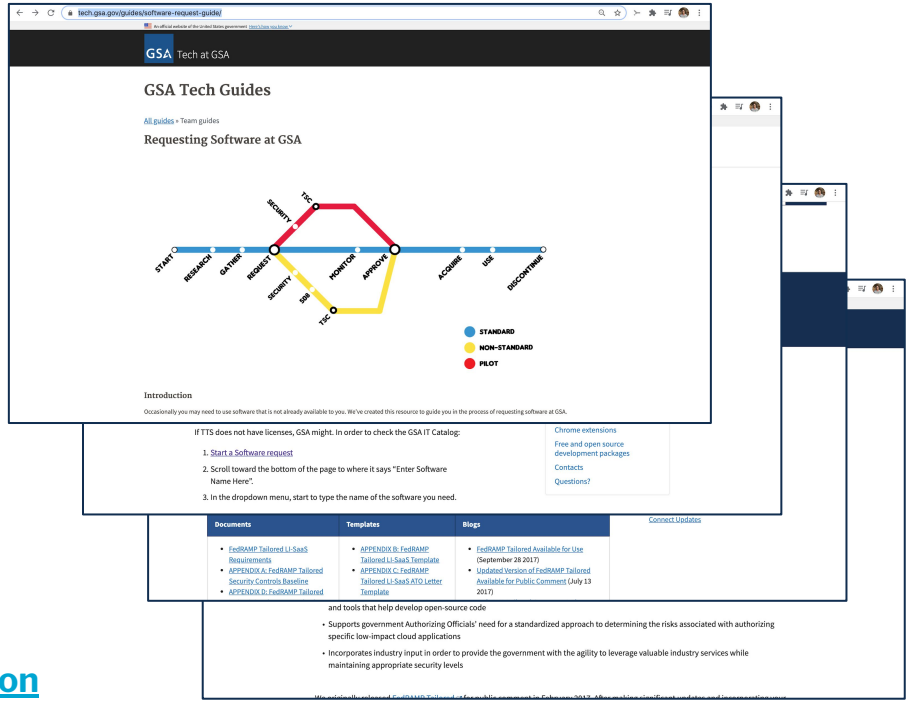
Objective

- Improve SaaS Authorization documentation
- Identify SaaS Auth pain points
- Propose potential solutions to streamline the process

SaaS Documentation Today

TECHNOLOGY TRANSFORMATION SERVICES

- 10k Software Handbook Page
- TTS SaaS Inventory List
- IT Standards Policy
- LiSaaS Policy
- LightSaaS Policy
- IT Security Procedural Guides
- Requesting Software at GSA
- FedRAMP Tailored
- Pursuing a FedRAMP Tailored Authorization



SaaS Expert Interviews

TECHNOLOGY TRANSFORMATION SERVICES

GSA

TTS

Within TTS, there are offices trying to do the similar thing or use a similar tool; they would like to know what others are doing or what has already been done before. There are a bunch of overlapping resources that have various levels of being: up-to-date, welcoming/intuitive, easy to navigate

- 18F Engineering, Design, Projects
- Presidential Innovation Fellows
- Login.gov
- Cloud.gov

FedRAMP

We would like to get insight into the FedRAMP process

- Customer Relations

GSA

TTS gets questions every few weeks or so from other agencies (and within GSA itself) along the lines of “we see you are using [modern tool]—but how??” or “I want to use [new tool]—what are the steps to doing so?” We do not have a comprehensive answer.

- GSA IT Security
- GSA IT CTO
- Enterprise Architecture

Vendors

It is difficult for vendors to understand: the steps of the process, what they need to do/provide and when, how long it will take, what it will cost them, etc

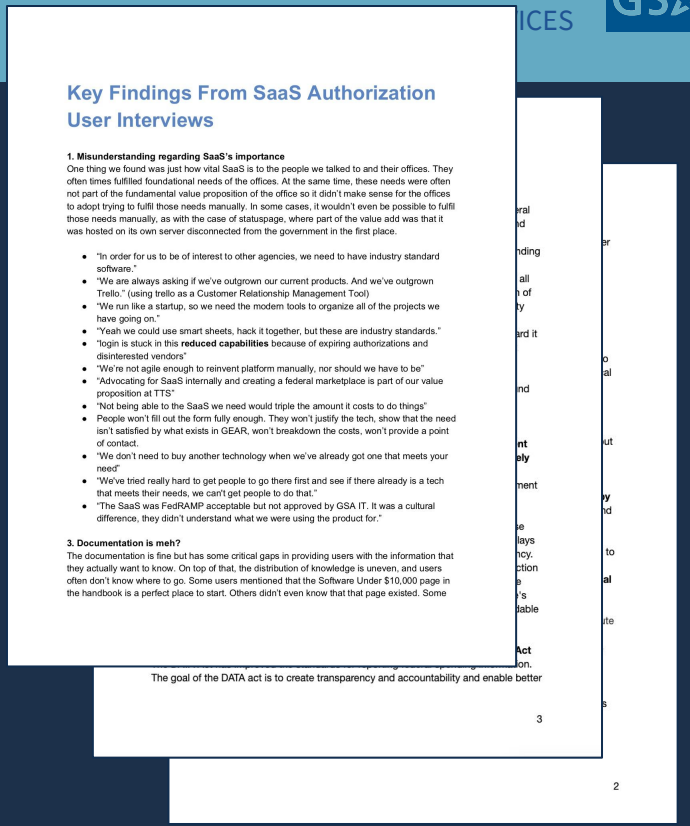
- Security Team
- Acquisitions Team

Phase I Findings

TECHNOLOGY TRANSFORMATION ICES

GSA

1. Lacking documentation
2. Miscommunication and disconnect between stakeholders
3. GEAR isn't trusted/used
4. No tracking
5. Catch 22 Problem
6. FedRAMP frustrations
7. Lots of passion around issue



Key Findings From SaaS Authorization User Interviews

1. Misunderstanding regarding SaaS's importance
One thing we found was just how vital SaaS is to the people we talked to and their offices. They often times fulfilled foundational needs of the offices. At the same time, these needs were often not part of the fundamental value proposition of the office so it didn't make sense for the offices to adopt trying to fulfil those needs manually. In some cases, it wouldn't even be possible to fulfil those needs manually, as with the case of statuspage, where part of the value add was that it was hosted on its own server disconnected from the government in the first place.

- "In order for us to be of interest to other agencies, we need to have industry standard software."
- "We are always asking if we've outgrown our current products. And we've outgrown Trello." (using trello as a Customer Relationship Management Tool)
- "We run like a startup, so we need the modern tools to organize all of the projects we have going on."
- "Yeah we could use smart sheets, hack it together, but these are industry standards."
- "login is stuck in this **reduced capabilities** because of expiring authorizations and disinterested vendors"
- "We're not agile enough to reinvent platform manually, nor should we have to be"
- "Advocating for SaaS internally and creating a federal marketplace is part of our value proposition at TTS"
- "Not being able to the SaaS we need would triple the amount it costs to do things"
- People won't fill out the form fully enough. They won't justify the tech, show that the need isn't satisfied by what exists in GEAR, won't breakdown the costs, won't provide a point of contact.
- "We don't need to buy another technology when we've already got one that meets your need"
- "We've tried really hard to get people to go there first and see if there already is a tech that meets their needs, we can't get people to do that."
- "The SaaS was FedRAMP acceptable but not approved by GSA IT. It was a cultural difference, they didn't understand what we were using the product for."

3. Documentation is meh?
The documentation is fine but has some critical gaps in providing users with the information that they actually want to know. On top of that, the distribution of knowledge is uneven, and users often don't know where to go. Some users mentioned that the Software Under $10,000 page in the handbook is a perfect place to start. Others didn't even know that that page existed. Some

The goal of the DATA act is to create transparency and accountability and enable better

3

2

Key ideas

TECHNOLOGY TRANSFORMATION SERVICES

GSA

1. Better tracking
2. Accurate Data
3. Simple Documentation
4. Dedicated Point of Contact

Lacking Documentation

There is no one definitive place to go for information, users don’t know about existing documentation, and existing documentation is missing key details.

I didn't know there was resources [like the Handbook] there that could help us

— TTS

Would have liked to know what the roles and responsibilities are, what the timelines are, how we can help outside of role and responsibility, and how much time and effort it would take

—TTS

We often get questions from agencies asking about other agencies' software and ATO

— FedRAMP

We didn't know what we needed to have going into the process. Maybe there was a link on the FedRAMP page, but it wasn't obvious.

— Vendor

Miscommunication and Disconnect

There is miscommunication and disconnect between authorization teams and requesters, authorization teams and vendors, and among authorization teams

Miscommunication Between Teams

About 20-30% of my time is spent responding to users asking for a security update and then tagging or bugging Security to get the update.

— CTO

Why can’t security be more open with its statuses? I wish that all the teams talked to one another. That's really my primary goal.

— CTO

There is confusion about what the pilot program even is. Some people call it a proof of concept where it does need to get reviewed, can host personal data, and can be put up on our server.

— CTO

Miscommunication With Requesters

People won't fill out the form. They won't justify the tech, show that the need isn't satisfied by what exists in GEAR, won't breakdown the costs, won't provide a point of contact.

— CTO

It was a cultural difference because they didn't know what we were using it for. We've said that if we don't get this product approved, we would just use Twitter for the same purposes.

— TTS

> We had to end up calling a meeting between us, the vendor, and GSA IT ourselves because the process had stalled. Both sides thought they were waiting on the other.
>
> — *TTS*

Miscommunication With Vendors

Vendors or users often don't follow up with the actions that are required of them at the end of the process.

— Security

Agencies customers have told us that they're not sure why they need Moderate (they just know they've been told that). Talking through the point of sale instead of security directly is like playing a game of telephone.

— Vendor

GEAR isn’t trusted or used

People are skeptical about the validity of the data in GEAR. This results in users not using it, either opting to message on Slack instead, or requesting duplicative software

GEAR is difficult for me because I don’t trust the validity of data. It feels out of date. If it doesn't have the answer I want, I just ask #infrastructure

— *TTS*

It’s fidgety, software is sometimes listed on a different name, sometimes the reseller was listed rather than the original equipment manufacturer

— *TTS*

I want to be able to make edits to the GEAR architecture. This is something we don't have any control over. We have to ask the EA team. I just want to clean up GEAR and display separately all approved tech, sunsetted, and denied. I also want to show in the comment section why it was denied.

— CTO

No tracking

Right now, there is no real way for GSA IT or anyone to track who is using what software or how to contact them. Relatedly, there is no way for users to express demand/interest for a certain software.

There's no way to see if other people have already requested, whether it be to prevent duplicate requests or allow users to reinforce desire/need for an existing request. All requests just get dumped into salesforce.

— Security

Sometimes there are cases where we don't approve a software because it is not critical, but once it is up on GEAR, someone starts using it and for them it is critical.

— Security

> When the approval expiration date comes, and we reach out to the champion. If the champion doesn't respond back, we cancel or deny that technology and remove it from the GEAR list. The problem is that we have no idea who else might be using it.
>
> *— CTO*

Catch 22

In order to buy licenses for a product, requesters need the vendor to go through the security process. However, vendors often don’t want to go through the process or send over any scans without a commitment from the offices to buy at least some amount of licenses.

A vendor wouldn't go through with the security process unless we committed to 50 licenses

— *TTS*

(People don't know about the Pilot Program. People didn't seem to mention it.)

FedRAMP frustrations

Vendors felt that going through the FedRAMP process felt subjective and inconsistent, with federal and office specific requirements not lining up, and there not being clear communication of requirements beforehand.

There was a disconnect between PMO requirements vs GSA requirements.

— *Vendor*

Going through the process, it felt like we were dealing with a moving target.

— *Vendor*

The problem was that we weren't given a list of what was needed from us up front.

— *Vendor*

For Tailored, the bar seemed to be higher than what others were looking for.

— Vendor

There was a lack of Consistency. Sometimes it would say that a certain control is no longer considered only for GSA to turn around and say that we do use that control.

— Vendor

Open Questions

Question 1

How do we improve communication throughout the process?

Question 2

How can we improve GEAR/data to make it more trustworthy?

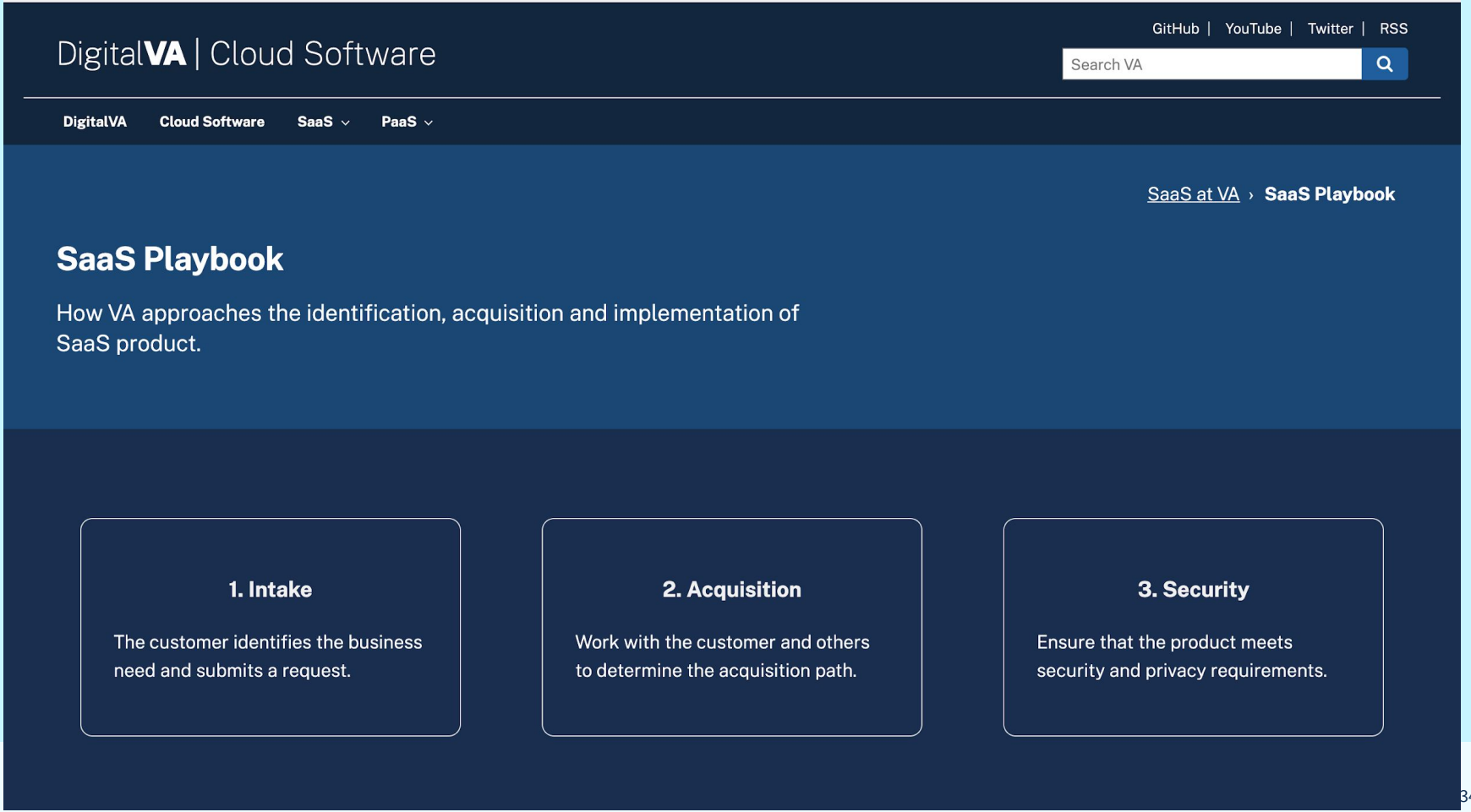
Question 3

How do we implement tracking?

Proposed Solutions

Stated Problems		Easy Solutions	Medium	Hard
Documentation	Lacking Scattered Convoluted	Update handbook to inlcude roles and responsibilities, timeline of the process, warning about the end steps, pilot program, and costs and effort	Create page like Veteran Affairs site (us or security) that include all of the key things identified	Create different forms of documentation such as a video, with visual queues. Have this be presented as part of onboarding or before going through the request process.
Communication with teams to users	Not clear Not condusive to dialogue Unsurity	Pin a slack post		Policy: SaaS representative
		Create a Slack Bot		Policy: More collaborative meetings. Regular SaaS check-ins between TTS, CTO, Security, and FedRAMP
Transparency	Lacking Not Trusted	Public checklist that Security uses		
		Policy: send out general timeline along with the checklist document to vendors		
Tracking	Lacking		Policy: create an avenue to advocate for tech after its been denied (maybe incorporate a comment system to have dialogue). Incorporate this with higher standard for acceptance (cost, justification, point of contact)	Create a mechanism for individuals/offices to easily indicate interest/use of a given tool (possibly on GEAR or ServiceNow)
			Display separately all approved, sunsetted, and denied tech. Show in the comment section why it was denied. Reorganize GEAR by demand (to make it more usable)	
Catch 22		Update handbook to inlcude roles and responsibilities, timeline of the process, warning about the end steps, pilot program, and costs and effort		Create a mechanism for individuals/offices to easily indicate interest/use of a given tool (possibly on GEAR or ServiceNow)
		Policy: send out general timeline along with the checklist document to vendors		Policy: make GSA more on hands at the beginning of the FedRAMP process for systems we are sponsoring

Veteran Affairs Site



Discussion
& questions